On the rank conjecture

Igor Nikolaev *

Abstract

A rank conjecture says that the rank of elliptic curve with complex multiplication is one less the so-called arithmetic complexity of corresponding noncommutative torus with real multiplication. We prove the conjecture for the $\mathbb{Q}$-curves introduced by B. H. Gross.

Key words and phrases: complex and real multiplication

MSC: 11G15 (complex multiplication); 46L85 (noncommutative topology)

1 Introduction

It was noticed some time ago, that there exists a fundamental duality between elliptic curves and certain (associative) operator algebras known as the noncommutative tori [6]. Such a duality is realized by a covariant functor F (the Teichmüller functor), which maps isomorphic elliptic curves to the stably isomorphic algebras [3]. The functor F is rather explicit; for instance, if elliptic curve, $\mathcal{E}_{CM}$, has complex multiplication by $\sqrt{-D}$, then the corresponding noncommutative torus, $\mathcal{A}_{RM}$, has real multiplication by $\sqrt{D}$, see Appendix for definition. A natural question arises about intrinsic invariants of $\mathcal{E}_{CM}$ expressed in terms of the torus $\mathcal{A}_{RM}$. The present article deals with one of such invariants – the rank of $\mathcal{E}_{CM}$ as function of the so-called arithmetic complexity of $\mathcal{A}_{RM}$ (to be defined in terms of the continued fraction of $\sqrt{D}$). Let us review some preliminary facts.

*Partially supported by NSERC.

Denote by $\mathbb{H} = \{x + iy \in \mathbb{C} \mid y > 0\}$ the upper half-plane and for $\tau \in \mathbb{H}$ let $\mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau)$ be a complex torus; we routinely identify the latter with a non-singular elliptic curve via the Weierstrass $\wp$ function [7], pp. 6-7. Recall that complex tori of (complex) moduli τ and τ' are isomorphic, whenever $\tau' = (a\tau + b)/(c\tau + d)$, where $a, b, c, d \in \mathbb{Z}$ and $ad - bc = 1$. If modulus τ is an imaginary quadratic number, then elliptic curve is said to have complex multiplication; in this case the endomorphism ring of lattice $L = \mathbb{Z} + \mathbb{Z}\tau$ is isomorphic to an order $\mathfrak{R}$ of conductor $f \geq 1$ in the quadratic field $\mathbb{Q}(\sqrt{-D})$, where $D \geq 1$ is a square-free integer [7], pp. 95-96. We shall denote such an elliptic curve by $\mathcal{E}_{CM}^{(-D,f)}$. The curve $\mathcal{E}_{CM}^{(-D,f)}$ is isomorphic to a non-singular cubic defined over the field $H = K(j(\mathcal{E}_{CM}^{(-D,f)}))$, where $K = \mathbb{Q}(\sqrt{-D})$ and $j(\mathcal{E}_{CM}^{(-D,f)})$ is the j-invariant of $\mathcal{E}_{CM}^{(-D,f)}$. The Mordell-Weil theorem says that the set of H-rational points of $\mathcal{E}_{CM}^{(-D,f)}$ is a finitely generated abelian group, whose rank we shall denote by $rk\ (\mathcal{E}_{CM}^{(-D,f)})$; for an exact definition of the rank, we refer the reader to [1], p. 49. The integer $rk\ (\mathcal{E}_{CM}^{(-D,f)})$ is an invariant of the isomorphism class of $\mathcal{E}_{CM}^{(-D,f)}$.

Denote by $(\mathcal{E}_{CM}^{(-D,f)})^\sigma$, $\sigma \in Gal\ (H|\mathbb{Q})$ the Galois conjugate of the curve $\mathcal{E}_{CM}^{(-D,f)}$; by a $\mathbb{Q}$-*curve* one understands $\mathcal{E}_{CM}^{(-D,f)}$, such that there exists an isogeny between $(\mathcal{E}_{CM}^{(-D,f)})^\sigma$ and $\mathcal{E}_{CM}^{(-D,f)}$ for each $\sigma \in Gal\ (H|\mathbb{Q})$. Let $\mathcal{E}(p) := \mathcal{E}_{CM}^{(-p,1)}$, where p is a prime number; then $\mathcal{E}(p)$ is a $\mathbb{Q}$-curve whenever $p = 3 \textbf{ mod } 4$ [1], p. 33. The set of all primes $p = 3 \textbf{ mod } 4$ will be denoted by $\mathfrak{P}_{3 \textbf{ mod } 4}$. The rank of $\mathcal{E}(p)$ is always divisible by $2h_K$, where h_K is the class number of field K; by a $\mathbb{Q}$-*rank* of $\mathcal{E}(p)$ we understand the integer $rk_{\mathbb{Q}}(\mathcal{E}(p)) := \frac{1}{2h_K}\ rk\ (\mathcal{E}(p))$.

Let $\mathcal{A}_{RM}^{(D,f)}$ be a torus with real multiplication by the order R of conductor $f \geq 1$ in the real quadratic field $\mathbb{Q}(\sqrt{D})$, see Appendix. The irrational number $\sqrt{D}$ unfolds in a periodic continued fraction; its minimal period we shall write as $(\overline{a_{k+1}, \ldots, a_{k+P}})$. In this period the entries a_i's are viewed as (discrete) variables; in general, due to a symmetry (special form) of quadratic irrationality, there are polynomial relations (constraints) between a_i so that some of them depend on the other, see Section 2. The total number of independent variables a_i's in $(\overline{a_{k+1}, \ldots, a_{k+P}})$ will be called an *arithmetic complexity* of $\mathcal{A}_{RM}^{(D,f)}$ and denoted by $c(\mathcal{A}_{RM}^{(D,f)})$; such a complexity is equal to the dimension of a connected component of affine variety given by the diophantine equation (5). It follows from definition, that $1 \leq c(\mathcal{A}_{RM}^{(D,f)}) \leq P$ and integer $c(\mathcal{A}_{RM}^{(D,f)})$ is an invariant of the stable isomorphism class of $\mathcal{A}_{RM}^{(D,f)}$.

Recall that the Teichmüller functor acts by the formula $F(\mathcal{E}_{CM}^{(-D,f)}) = \mathcal{A}_{RM}^{(D,f)}$, see lemma 6. By a *rank conjecture* one understands the following equation relating the rank of $\mathcal{E}_{CM}^{(-D,f)}$ to the complexity of $\mathcal{A}_{RM}^{(D,f)}$.

Conjecture 1 **([3])** $\qquad rk\ (\mathcal{E}_{CM}^{(-D,f)}) + 1 = c(\mathcal{A}_{RM}^{(D,f)}).$

In the sequel, we shall restrict conjecture 1 to the $\mathbb{Q}$-curves $\mathcal{E}(p)$; in view of this additional symmetry, the initial rank of $\mathcal{E}(p)$ must be divided by $2h_K$. Thus, one gets the following refinement of conjecture 1.

Conjecture 2 **($\mathbb{Q}$-rank conjecture)**

$$\frac{1}{2h_K}\ rk\ (\mathcal{E}(p)) + 1 = c(\mathcal{A}_{RM}^{(p,1)}).$$

The aim of present note is to verify the $\mathbb{Q}$-rank conjecture for primes $p = 3$ **mod** 4; our main result can be expressed as follows.

Theorem 1 *For each prime* $p = 3$ **mod** 4 *the* $\mathbb{Q}$*-rank conjecture is true.*

The article is organized as follows. The arithmetic complexity is defined in Section 2. Theorem 1 is proved in Section 3. In Section 4 we illustrate theorem 1 by examples of $\mathcal{E}(p)$ for primes under 100. A brief review of the algebras $\mathcal{A}_\theta$ and functor F can be found in Section 5.

2 Arithmetic complexity

Let θ be a quadratic irrationality, i.e. irrational root of a quadratic polynomial $ax^2+bx+c=0$, where $a,b,c\in\mathbb{Z}$; denote by $Per\ (\theta) := (\overline{a_1, a_2, \dots, a_P})$ the minimal period of continued fraction of θ taken up to a cyclic permutation. Fix P and suppose for a moment that θ is a function of its period:

$$\theta(x_0, x_1, \dots, x_P) = [x_0, \overline{x_1, \dots, x_P}], \tag{1}$$

where $x_i \ge 1$ are integer variables; then $\theta(x_0,\dots,x_P)\in\mathbb{Q}+\sqrt{\mathbb{Q}}$, where $\sqrt{\mathbb{Q}}$ are square roots of positive rationals. Consider a constraint (a restriction) $x_1 = x_{P-1}, x_2 = x_{P-2}, \dots, x_P = 2x_0$; then $\theta(x_0, x_1, x_2, \dots, x_2, x_1, 2x_0) \in \sqrt{\mathbb{Q}}$, see e.g. [4], p. 79. Notice, that in this case there are $\frac{1}{2}P+1$ independent variables, if P is even and $\frac{1}{2}(P+1)$, if P is odd. The number of independent variables will further decrease, if θ is square root of an integer; let us introduce

some notation. For a regular fraction $[a_0, a_1, \ldots]$ one associates the linear equations

$$\begin{cases} y_0 &= a_0 y_1 + y_2 \\ y_1 &= a_1 y_2 + y_3 \\ y_2 &= a_2 y_3 + y_4 \\ &\vdots \end{cases} \tag{2}$$

One can put equations (2) in the form

$$\begin{cases} y_j &= A_{i-1,j} y_{i+j} + a_{i+j} A_{i-2,j} y_{i+j+1} \\ y_{j+1} &= B_{i-1,j} y_{i+j} + a_{i+j} B_{i-2,j} y_{i+j+1}, \end{cases} \tag{3}$$

where the polynomials $A_{i,j}, B_{i,j} \in \mathbb{Z}[a_0, a_1, \ldots]$ are called Muir's symbols [4], p.10. The following well-known lemma will play an important rôle.

Lemma 1 ([4], pp. 88 and 107) *There exists a square-free integer $D > 0$, such that*

$$[x_0, \overline{x_1, \ldots, x_1, x_P}] = \begin{cases} \sqrt{D}, & \text{if } x_P = 2x_0 \text{ and } D = 2, 3 \textbf{ mod } 4, \\ \frac{\sqrt{D}+1}{2}, & \text{if } x_P = 2x_0 - 1 \text{ and } D = 1 \textbf{ mod } 4, \end{cases} \tag{4}$$

if and only if x_P satisfies the diophantine equation

$$x_P = m A_{P-2,1} - (-1)^P A_{P-3,1} B_{P-3,1}, \tag{5}$$

for an integer $m > 0$; moreover, in this case $D = \frac{1}{4} x_P^2 + m A_{P-3,1} - (-1)^P B_{P-3,1}^2$.

Let $(x_0^*, \ldots, x_P^*)$ be a solution of the diophantine equation (5). By *dimension*, d, of this solution one understands the maximal number of variables x_i, such that for every $s \in \mathbb{Z}$ there exists a solution of (5) of the form $(x_0, \ldots, x_i^* + s, \ldots, x_P)$. In geometric terms, d is equal to dimension of a connected component through the point $(x_0^*, \ldots, x_P^*)$ of an affine variety V_m (i.e. depending on m) defined by equation (5). Let us consider a simple

Example 1 ([4], p. 90) If $P = 4$, then Muir's symbols are: $A_{P-3,1} = A_{1,1} = x_1 x_2 + 1$, $B_{P-3,1} = B_{1,1} = x_2$ and $A_{P-2,1} = A_{2,1} = x_1 x_2 x_3 + x_1 + x_3 = x_1^2 x_2 + 2x_1$, since $x_3 = x_1$. Thus, equation (5) takes the form:

$$2x_0 = m(x_1^2 x_2 + 2x_1) - x_2(x_1 x_2 + 1), \tag{6}$$

and, therefore, $\sqrt{x_0^2 + m(x_1 x_2 + 1) - x_2^2} = [x_0, \overline{x_1, x_2, x_1, 2x_0}]$. First, let us show that the affine variety defined by equation (6) is not connected. Indeed,

by lemma 1, parameter m must be integer for all (integer) values of x_0, x_1 and x_2. This is not possible in general, since from (6) one obtains $m = (2x_0+x_2(x_1x_2+1))(x_1^2x_2+2x_1)^{-1}$ is a rational number. However, a restriction to $x_1 = 1,\ x_2 = x_0 - 1$ defines a (maximal) connected component of variety (6), since in this case $m = x_0$ is always an integer. Thus, one gets a family of solutions of (6) of the form $\sqrt{(x_0+1)^2-2} = [x_0, \overline{1, x_0-1, 1, 2x_0}]$, where each solution has dimension $d = 1$. (We shall use this solution in the next section.)

Definition 1 *By an arithmetic complexity of* $\mathcal{A}_{RM}^{(D,1)}$ *one understands the dimension of solution* $(x_0^*, \ldots, x_P^*)$ *of the diophantine equation* [1] *:*

$$\frac{1}{4}x_P^2 + mA_{P-3,1} - (-1)^P B_{P-3,1}^2 = D,$$

see lemma 1 for the notation. The complexity equals infinity, if and only if, torus has no real multiplication.

Remark 1 In [3] the arithmetic complexity was defined as the maximal number of independent variables, i.e. $d = P$ the length of the period. It is easy to see, that these two definitions coincide on the generic [2] tori with real multiplication.

3 Proof of theorem 1

We shall split the proof in a series of lemmas starting with the following

Lemma 2 *If* $[x_0, \overline{x_1, \ldots, x_k, \ldots, x_1, 2x_0}] \in \sqrt{\mathfrak{P}_{3 \textbf{ mod } 4}}$ *, then:*

(i) $P = 2k$ *is an even number, such that:*

(a) $P \equiv 2 \textbf{ mod } 4$*, if* $p \equiv 3 \textbf{ mod } 8$*;*

(b) $P \equiv 0 \textbf{ mod } 4$*, if* $p \equiv 7 \textbf{ mod } 8$*;*

(ii) either of two is true:

(a) $x_k = x_0$ *(a culminating period);*

(b) $x_k = x_0 - 1$ *and* $x_{k-1} = 1$ *(an almost-culminating period).*

[1]This equation can be replaces by the equivalent equation (5).

[2]I.e. a torus with real multiplication, such that $\theta = r_1 + r_2\sqrt{D}$, where r_1 and r_2 are arbitrary rational numbers.

Proof. (i) Recall that if $p \neq 2$ is a prime, then one and only one of the following diophantine equations is solvable:

$$\left\{\begin{array}{lll} x^2 - py^2 & = & -1, \\ x^2 - py^2 & = & 2, \\ x^2 - py^2 & = & -2, \end{array}\right. \tag{7}$$

see e.g. [4], Satz 3.21. Since $p \equiv 3 \ \mathbf{mod}\ 4$, one concludes that $x^2 - py^2 = -1$ is not solvable [4], Satz 3.23-24; this happens if and only if $P = 2k$ is even (for otherwise the continued fraction of $\sqrt{p}$ would provide a solution).

It is known, that for even periods $P = 2k$ the convergents A_i/B_i satisfy the diophantine equation $A_{k-1}^2 - pB_{k-1}^2 = (-1)^k\ 2$, see [4], p.103; thus if $P \equiv 0 \ \mathbf{mod}\ 4$, the equation $x^2 - py^2 = 2$ is solvable and if $P \equiv 2 \ \mathbf{mod}\ 4$, then the equation $x^2 - py^2 = -2$ is sovable. But equation $x^2 - py^2 = 2$ (equation $x^2 - py^2 = -2$, resp.) is solvable if and only if $p \equiv 7 \ \mathbf{mod}\ 8$ ($p \equiv 3 \ \mathbf{mod}\ 8$, resp.), see [4], Satz 3.23 (Satz 3.24, resp.). Item (i) follows.

(ii) The equation $A_{k-1}^2 - pB_{k-1}^2 = (-1)^k\ 2$ is a special case of equation $A_{k-1}^2 - pB_{k-1}^2 = (-1)^k\ Q_k$, where Q_k is the full quotient of continued fraction [4], p.92; therefore, $Q_k = 2$. One can now apply Satz 3.15 of [4], which says that for $P = 2k$ and $Q_k = 2$ the continued fraction of $\sqrt{\mathfrak{P}_{3\ \mathbf{mod}\ 4}}$ is either culminating (i.e. $x_k = x_0$) or almost-culminating (i.e. $x_k = x_0 - 1$ and $x_{k-1} = 1$). Lemma 2 follows. $\square$

Lemma 3 *If $p \equiv 3 \ \mathbf{mod}\ 8$, then $c(\mathcal{A}_{RM}^{(p,1)}) = 2$.*

Proof. The proof proceeds by induction in period P, which is in this case $P \equiv 2 \ \mathbf{mod}\ 4$ by lemma 2. We shall start with $P = 6$, since $P = 2$ reduces to it, see item (i) below.

(i) Let $P = 6$ be a culminating period; then equation (5) admits a general solution $[x_0, \overline{x_1, 2x_1, x_0, , 2x_1, x_1, 2x_0}] = \sqrt{x_0^2 + 4nx_1 + 2}$, where $x_0 = n(2x_1^2 + 1) + x_1$, see [4], p. 101. The solution depends on two integer variables x_1 and n, which is the maximal possible number of variables in this case; therefore, the dimension of the solution is $d = 2$, so as complexity of the corresponding torus. Notice that the case $P = 2$ is obtained from $P = 6$ by restriction to $n = 0$; thus the complexity for $P = 2$ is equal to 2.

(ii) Let $P = 6$ be an almost-culminating period; then equation (5) has a solution $[3s + 1, \overline{2, 1, 3s, 1, 2, 6s + 2}] = \sqrt{(3s + 1)^2 + 2s + 1}$, where s is an

integer variable [4], p. 103. We encourage the reader to verify, that this solution is a restriction of solution (i) to $x_1 = -1$ and $n = s + 1$; thus, the dimension of our solution is $d = 2$, so as the complexity of the corresponding torus.

(iii) Suppose a solution $[x_0, \overline{x_1, \ldots, x_{k-1}, x_k, x_{k-1}, \ldots, x_1, 2x_0}]$ with the (culminating or almost-culminating) period $P_0 \equiv 3$ **mod** 8 has dimension $d = 2$; let us show that a solution

$$[x_0, \overline{y_1, x_1, \ldots, x_{k-1}, y_{k-1}, x_k, y_{k-1}, x_{k-1}, \ldots, x_1, y_1, 2x_0}] \tag{8}$$

with period $P_0 + 4$ has also dimension $d = 2$. According to Weber [8], if (8) is a solution to the diophantine equation (5), then either (i) $y_{k-1} = 2y_1$ or (ii) $y_{k-1} = 2y_1 + 1$ and $x_1 = 1$. We proceed by showing that case (i) is not possible for the square roots of prime numbers.

Indeed, let to the contrary $y_{k-1} = 2y_1$; then the following system of equations must be compatible:

$$\left\{ \begin{array}{lcl} A_{k-1}^2 & - & pB_{k-1}^2 = -2, \\ A_{k-1} & = & 2y_1 A_{k-2} + A_{k-3}, \\ B_{k-1} & = & 2y_1 B_{k-2} + B_{k-3}, \end{array} \right. \tag{9}$$

where A_i, B_i are convergents and the first equation is solvable since $p \equiv 3$ **mod** 8. From the first equation, both convergents A_{k-1} and B_{k-1} are odd numbers. (They are both odd or even, but even excluded, since A_{k-1} and B_{k-1} are relatively prime.) From the last two equations, the convergents A_{k-3} and B_{k-3} are also odd. Then the convergents A_{k-2} and B_{k-2} must be even, since among six consequent convergents $A_{k-1}, B_{k-1}, A_{k-2}, B_{k-2}, A_{k-3}, B_{k-3}$ there are always two even; but this is not possible, because A_{k-2} and B_{k-2} are relatively prime. Thus, $y_{k-1} \neq 2y_1$.

Therefore (8) is a solution of the diophantine equation (5) if and only if $y_{k-1} = 2y_1 + 1$ and $x_1 = 1$; the dimension of such a solution coincides with the dimension of solution $[x_0, \overline{x_1, \ldots, x_{k-1}, x_k, x_{k-1}, \ldots, x_1, 2x_0}]$, since for two new integer variables y_1 and y_{k-1} one gets two new constraints. Thus, the dimension of solution (8) is $d = 2$, so as the complexity of the corresponding torus. Lemma 3 follows. □

Lemma 4 *If* $p \equiv 7$ **mod** 8, *then* $c(\mathcal{A}_{RM}^{(p,1)}) = 1$.

Proof. The proof proceeds by induction in period $P \equiv 0$ **mod** 4, see lemma 2; we start with $P = 4$.

(i) Let $P = 4$ be a culminating period; then equation (5) admits a solution $[x_0, \overline{x_1, x_2, x_1, 2x_0}] = \sqrt{x_0^2 + m(x_1 x_2 + 1) - x_2^2}$, where $x_2 = x_0$, see example 1 for the details. Since the polynomial $m(x_0 x_1 + 1)$ under the square root represents a prime number, we have $m = 1$; the latter equation is not solvable in integers x_0 and x_1, since $m = x_0(x_0 x_1 + 3) x_1^{-1} (x_0 x_1 + 2)^{-1}$. Thus, there are no solutions of (5) with the culminating period $P = 4$.

(ii) Let $P = 4$ be an almost-culminating period; then equation (5) admits a solution $[x_0, \overline{1, x_0 - 1, 1, 2x_0}] = \sqrt{(x_0 + 1)^2 - 2}$. The dimension of this solution was proved to be $d = 1$, see example 1; thus, the complexity of the corresponding torus is equal to 1.

(iii) Suppose a solution $[x_0, \overline{x_1, \dots, x_{k-1}, x_k, x_{k-1}, \dots, x_1, 2x_0}]$ with the (culminating or almost-culminating) period $P_0 \equiv 7 \ \mathbf{mod}\ 8$ has dimension $d = 1$. It can be shown by the same argument as in lemma 3, that for a solution of the form (8) having the period $P_0 + 4$ the dimension remains the same, i.e. $d = 1$; we leave details to the reader. Thus, complexity of the corresponding torus is equal to 1. Lemma 4 follows. $\square$

Lemma 5 ([1], p.78)

$$\frac{1}{2h_K}\ rk\ (\mathcal{E}(p)) = \begin{cases} 1, & if\ \ p \equiv 3 \ \mathbf{mod}\ 8 \\ 0, & if\ \ p \equiv 7 \ \mathbf{mod}\ 8. \end{cases} \tag{10}$$

Theorem 1 follows from lemma 6 and lemmas 3-5. $\square$

4 Examples

The table below illustrates theorem 1 for all $\mathbb{Q}$-curves $\mathcal{E}(p)$, such that $p < 100$; notice, that in general there are infinitely many pairwise non-isomorphic $\mathbb{Q}$-curves [1].

$p \equiv 3$ **mod** 4	$rk_{\mathbb{Q}}(\mathcal{E}(p))$	$\sqrt{p}$	$c(\mathcal{A}_{RM}^{(p,1)})$
3	1	$[1, \overline{1, 2}]$	2
7	0	$[2, \overline{1, 1, 1, 4}]$	1
11	1	$[3, \overline{3, 6}]$	2
19	1	$[4, \overline{2, 1, 3, 1, 2, 8}]$	2
23	0	$[4, \overline{1, 3, 1, 8}]$	1
31	0	$[5, \overline{1, 1, 3, 5, 3, 1, 1, 10}]$	1
43	1	$[6, \overline{1, 1, 3, 1, 5, 1, 3, 1, 1, 12}]$	2
47	0	$[6, \overline{1, 5, 1, 12}]$	1
59	1	$[7, \overline{1, 2, 7, 2, 1, 14}]$	2
67	1	$[8, \overline{5, 2, 1, 1, 7, 1, 1, 2, 5, 16}]$	2
71	0	$[8, \overline{2, 2, 1, 7, 1, 2, 2, 16}]$	1
79	0	$[8, \overline{1, 7, 1, 16}]$	1
83	1	$[9, \overline{9, 18}]$	2

Figure 1: The $\mathbb{Q}$-curves $\mathcal{E}(p)$ with $p < 100$.

5 Appendix

Let $0 < \theta < 1$ be an irrational number; by a *noncommutative torus* $\mathcal{A}_\theta$ one understands the universal C^*-algebra generated by the unitaries u and v satisfying the commutation relation $vu = e^{2\pi i\theta}uv$ [5], [6]. The algebras $\mathcal{A}_\theta$ and $\mathcal{A}_{\theta'}$ are said to be stably isomorphic (Morita equivalent) if $\mathcal{A}_\theta \otimes \mathcal{K} \cong \mathcal{A}_{\theta'} \otimes \mathcal{K}$, where $\mathcal{K}$ is the C^*-algebra of compact operators; in this case $\theta' = (a\theta + b)/(c\theta + d)$, where $a, b, c, d \in \mathbb{Z}$ and $ad - bc = 1$.

The K-theory of $\mathcal{A}_\theta$ is Bott periodic with $K_0(\mathcal{A}_\theta) = K_1(\mathcal{A}_\theta) \cong \mathbb{Z}^2$; the range of trace on projections of $\mathcal{A}_\theta \otimes \mathcal{K}$ is a subset $\Lambda = \mathbb{Z} + \mathbb{Z}\theta$ of the real line, which is called a pseudo-lattice [2]. The torus $\mathcal{A}_\theta$ has *real multiplication*, if θ is a quadratic irrationality; in this case the endomorphism ring of pseudo-lattice Λ is isomorphic to an order R of conductor $f \geq 1$ in the real quadratic $\mathbb{Q}(\sqrt{D})$, where $D > 1$ is a square-free integer. The corresponding noncommutative torus we shall write as $\mathcal{A}_{RM}^{(D,f)}$.

There exists a covariant functor between elliptic curves and noncommutative tori; the functor maps isomorphic elliptic curves to the stably isomorphic

tori [3]. To give an idea, let ϕ be a closed form on a topological torus; the trajectories of ϕ define a measured foliation on the torus. By the Hubbard-Masur theorem, such a foliation corresponds to a point $\tau \in \mathbb{H}$. The map $F : \mathbb{H} \to \partial\mathbb{H}$ is defined by the formula $\tau \mapsto \theta = \int_{\gamma_2} \phi / \int_{\gamma_1} \phi$, where γ_1 and γ_2 are generators of the first homology of the torus. The following is true: (i) $\mathbb{H} = \partial\mathbb{H} \times (0, \infty)$ is a trivial fiber bundle, whose projection map coincides with F; (ii) F is a functor, which maps isomorphic complex tori to the stably isomorphic noncommutative tori. We shall refer to F as the *Teichmüller functor*; such a functor maps elliptic curves with complex multiplication to the noncommutative tori with real multiplication, *ibid.* The following lemma gives an explicit formula for F.

Lemma 6 *The functor F acts by the formula $\mathcal{E}_{CM}^{(-D,f)} \mapsto \mathcal{A}_{RM}^{(D,f)}$.*

Proof. Let L_{CM} be a lattice with complex multiplication by an order $\mathfrak{R} = \mathbb{Z} + (f\omega)\mathbb{Z}$ in the imaginary quadatic field $\mathbb{Q}(\sqrt{-D})$; the multiplication by $\alpha \in \mathfrak{R}$ generates an endomorphism $(a, b, c, d) \in M_2(\mathbb{Z})$ of the lattice L_{CM}. We shall use an explicit formula for the Teichmüller functor F ([3], p.524):

$$F : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in End\ (L_{CM}) \longmapsto \begin{pmatrix} a & b \\ -c & -d \end{pmatrix} \in End\ (\Lambda_{RM}), \tag{11}$$

where Λ_{RM} is the pseudo-lattice with real multiplication corresponding to L_{CM}. Moreover, one can always assume $d = 0$ in a proper basis of L_{CM}.

It is known, that $\Lambda_{RM} \subseteq R$, where $R = \mathbb{Z} + (f\omega)\mathbb{Z}$ is an order in the real quadratic number field; here $f \geq 1$ is the conductor of R and

$$\omega = \begin{cases} \frac{\sqrt{D}+1}{2} & \text{if } D \equiv 1 \textbf{ mod } 4, \\ \sqrt{D} & \text{if } D \equiv 2, 3 \textbf{ mod } 4. \end{cases} \tag{12}$$

We have to consider the following two cases.

Case I. If $D \equiv 1$ **mod** 4 then $\mathfrak{R} = \mathbb{Z} + (\frac{f+\sqrt{-f^2D}}{2})\mathbb{Z}$; thus the multiplier $\alpha = \frac{2m+fn}{2} + \sqrt{\frac{-f^2Dn^2}{4}}$ for some $m, n \in \mathbb{Z}$. Therefore multiplication by α corresponds to an endomorphism $(a, b, c, 0) \in M_2(\mathbb{Z})$, where

$$\begin{cases} a &= \quad Tr(\alpha) = \alpha + \bar{\alpha} = 2m + fn \\ b &= \quad -1 \\ c &= \quad N(\alpha) = \alpha\bar{\alpha} = \left(\frac{2m+fn}{2}\right)^2 + \frac{f^2Dn^2}{4}. \end{cases} \tag{13}$$

To calculate a primitive generator of endomorphisms of the lattice L_{CM} one should find a multiplier $\alpha_0 \neq 0$ such that

$$|\alpha_0| = \min_{m.n\in\mathbb{Z}} |\alpha| = \min_{m.n\in\mathbb{Z}} \sqrt{N(\alpha)}. \tag{14}$$

From the last equation of (13) the minimum is attained for $m = -\frac{f}{2}$ and $n = 1$ if f is even or $m = -f$ and $n = 2$ if f is odd. Thus

$$\alpha_0 = \begin{cases} \pm\frac{f}{2}\sqrt{-D}, & \text{if } f \text{ is even} \\ \pm f\sqrt{-D}, & \text{if } f \text{ is odd.} \end{cases} \tag{15}$$

To find the matrix form of the endomorphism α_0, we shall substitute in (11) $a = d = 0, b = -1$ and $c = \frac{f^2D}{4}$ if f is even or $c = f^2D$ if f is odd. Thus the Teichmüller functor maps the multiplier α_0 into

$$F(\alpha_0) = \begin{cases} \pm\frac{f}{2}\sqrt{D}, & \text{if } f \text{ is even} \\ \pm f\sqrt{D}, & \text{if } f \text{ is odd.} \end{cases} \tag{16}$$

Comparing equations (15) and (16) one verifies that formula $F(\mathcal{E}_{CM}^{(-D,f)}) = \mathcal{A}_{RM}^{(D,f)}$ is true in this case.

Case II. If $D \equiv 2$ or $3 \ \mathbf{mod}\ 4$ then $\mathfrak{R} = \mathbb{Z} + (\sqrt{-f^2D})\,\mathbb{Z}$; thus the multiplier $\alpha = m + \sqrt{-f^2Dn^2}$ for some $m, n \in \mathbb{Z}$. A multiplication by α corresponds to an endomorphism $(a, b, c, 0) \in M_2(\mathbb{Z})$, where

$$\begin{cases} a &= \quad Tr(\alpha) = \alpha + \bar{\alpha} = 2m \\ b &= \quad -1 \\ c &= \quad N(\alpha) = \alpha\bar{\alpha} = m^2 + f^2Dn^2. \end{cases} \tag{17}$$

We shall repeat the argument of Case I; then from the last equation of (17) the minimum of $|\alpha|$ is attained for $m = 0$ and $n = \pm 1$. Thus $\alpha_0 = \pm f\sqrt{-D}$.

To find the matrix form of the endomorphism α_0 we substitute in (11) $a = d = 0, b = -1$ and $c = f^2D$. Thus the Teichmüller functor maps the multiplier $\alpha_0 = \pm f\sqrt{-D}$ into $F(\alpha_0) = \pm f\sqrt{D}$. In other words, formula $F(\mathcal{E}_{CM}^{(-D,f)}) = \mathcal{A}_{RM}^{(D,f)}$ is true in this case as well.

Since all possible cases are exhausted, lemma 6 is proved. $\square$

References

[1] B. H. Gross, Arithmetic on Elliptic Curves with Complex Multiplication, Lecture Notes Math. 776 (1980), Springer.

[2] Yu. I. Manin, Real multiplication and noncommutative geometry, in "Legacy of Niels Hendrik Abel", 685-727, Springer, 2004.

[3] I. Nikolaev, Remark on the rank of elliptic curves, Osaka J. Math. 46 (2009), 515-527.

[4] O. Perron, Die Lehre von den Kettenbrüchen, Bd.1, Teubner, 1954.

[5] M. A. Rieffel, C^*-algebras associated with irrational rotations, Pacific J. of Math. 93 (1981), 415-429.

[6] M. A. Rieffel, Non-commutative tori – a case study of non-commutative differentiable manifolds, Contemp. Math. 105 (1990), 191-211. Available http://math.berkeley.edu/∼rieffel/

[7] J. H. Silverman, Advanced Topics in the Arithmetic of Elliptic Curves, GTM 151, Springer 1994.

[8] K. Weber, Kettenbrüche mit kulminierenden und fastkuminierenden Perioden, Sitzungsber. der Bayer. Akademie d. Wissenschaften zu München, mathemat.-naturwissen. Abteilung (1926), 41-62.

The Fields Institute for Mathematical Sciences, Toronto, ON, Canada, E-mail: igor.v.nikolaev@gmail.com

Current address: 616-315 Holmwood Ave., Ottawa, ON, Canada, K1S 2R2